UTILITY PATENT APPLICATION TRANSMITTAL

(for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	113306	Total Pages	21

First Named Inventor or Application Identifier

Arturo Maria

Express Mail Label No.	EM365589955US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:
Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

1. ☒ Fee Transmittal Form
   (submit an original, and a duplicate for fee processing)
2. ☒ Specification   [Total Pages 11]
   (preferred arrangement set forth below)
   – Descriptive title of invention
   – Cross References to Related Applications
   – Statement Regarding Fed sponsored R&D
   – Reference to Microfiche Appendix
   – Background of the Invention
   – Brief Summary of the Invention
   – Brief Description of the Drawings(if filed)
   – Detailed Description
   – Claim(s)
   – Abstract of the Disclosure
3. ☒ Drawing(s)(35 USC 113) [Total Sheets 3]
4. Oath or Declaration   [Total Pages 2]
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application(37 CFR 1.63(d))
   (for continuation/divisional with Box 17 completed)
   [Note Box 5 below]
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 163(d)(2) and 1.33(b)
5. ☐ Incorporation by reference(useable if Box 4b is checked)
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference herein.

6. ☐ Microfiche Computer Program *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission
   (if applicable, all necessary)
   a. ☐ Computer Readable Copy
   b. ☐ Paper Copy(identical to computer copy)
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers(cover sheet & document(s))
9. ☐ 37 CFR 3.73(b)Statement ☐ Power of Attorney
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure ☐ Copies of IDS
    Statement(IDS)/PTO-1449   Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
    (Should be specifically itemized)
14. ☐ Small Entity ☐ Statement filed in prior application,
    Statement(s)   Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
    (if foreign priority is claimed)
16. ☐ Other :

---

17. If a **CONTINUING APPLICATION**, *check appropriate box and supply the requisite information:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior Application No:
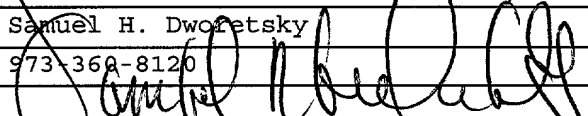
---

18. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* (Insert Customer No. or Attach bar code label here) or ☒ *Correspondence address below*

NAME	Samuel H. Dworetsky		
ADDRESS	AT&T CORP. P.O. Box 4110		
CITY	Middletown	STATE	New Jersey
		ZIP CODE	07748-4801
COUNTRY	United States of America	FAX	732-957-5505

19. SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

NAME	Samuel H. Dworetsky	Reg. #	27873
TELEPHONE	973-360-8120		
SIGNATURE		DATE	May 19, 1999

"Express Mail" Mailing Label Number   EM365589955US

Date of Deposit 5/19/99

I hereby certify that this application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington D.C. , 20231

Dino DiGangi
(Printed Name of Person Mailing Paper)

(Signature of Person Mailing Paper)

SYSTEM FOR SECURING INBOUND AND OUTBOUND
DATA PACKET FLOW IN A COMPUTER NETWORK

5   Cross Reference to Related Application

The present invention claims priority to provisional application Serial
No. 60/113,495 entitled "System for Securing Inbound and Outbound Data
Packet Flow in a Computer Network", the entire disclosure of which is hereby
incorporated by reference.

10

Technical Field

The present invention is directed to a method and apparatus for providing
authorization to access network resources.   More specifically, the present
invention is directed to a method and apparatus for providing an improved
15   authorization process for accessing network resources.

Background of the Invention

The ways in which people exchange information have been dramatically
changed by the continued evolution of data communication capabilities. Today,
20   more and more individuals have access to data networks by which they obtain
news, entertainment and business information. In fact, as the data communication
capabilities have increased, commerce along the data communication networks
has appeared and increased as well. Today, the wide area network commonly
referred   to   as   the   Internet   provides   its   users   with   access   to   almost
25   incomprehensible amounts of information.

FIG. 1 shows, in a schematic way, a network orientation in which a user 10
may attempt to get information from servers 15 and 20 via a wide area network
(WAN) 50. In this arrangement the user, via a terminal device such as a PC 60,
can connect to a gateway into the wide area network, here shown as Internet
30   service provider (ISP) 40. Typically, the user's terminal facility is connected to
the ISP via a standard telephone network 30 such as the Public Switched
Telephone Network (PSTN). Other configurations are possible where direct

connections into the ISP or into the wide area network are available. In this arrangement either one of the servers, or both, may desire to either charge for access to the information on the server or limit the access to information on the server based on some predetermined criteria. For example, the server 1, 12, may

5 provide an on-line version of a particular publication. The producer of the publication may desire to limit access to the publication to only those users willing to pay a subscription fee for the publication. Whenever the server decides to limit access to its resources, it must provide some facility by which it can authorize and/or authenticate a user who wishes to access a given resource.

10 Typically today, each server that wishes to limit access to its resources must also provide a separate authentication/authorization facility. This is represented in each of the servers illustrated in FIG. 1. This arrangement creates a tremendous burden for those who wish to limit access to the resources. As the number of subscribers grows, the authentication and authorization facility resource for each

15 server must be adapted to this growth. It also requires each individual who wishes to limit access to somehow incorporate additionally complex application software at additional cost to limit the access in the manner desired.

One alternative to this configuration has been presented by enCOMMERCE with an authorization program referred to as GetAccess. In this

20 arrangement, a centralized server includes an authorization database. Even though some of the facilities are centralized, each location interacting with GetAccess requires its own server to load a GetAccess interface and to communicate with the central facility in such a manner as to build its own authorization table with the aid of the centralized facility. While this off-loads some of the responsibility for

25 some of the authorization, it still requires complex interactions between the end servers and the centralized authority as well as the loading of authorization information at individual servers that are seeking to limit access to their resources.

It would be desirable to provide a technique by which the end point service providers or resource providers could off-load substantially all responsibility for

30 authorizing and authenticating access-requesting users in a manner which does not overly tax the resource providers or the communication network.

Summary of the Invention

The present invention provides a method for controlling access to network resources by allowing prospective users to assume the identities of pre-authorized machines. In accordance with an embodiment of the present invention, a user

5   seeking access to a particular network resource connects to a stateful virtual identity machine (SVIM). The machine is capable of authorizing the end user. The machine, having authorized an end user, shares its identity with the end user. As a consequence, the authorized user assumes the identity of the machine and appears to the network as if it were that machine. Since the network resource in

10   question has pre-authorized a machine, this pre-authorization extends to each end user that assumes the virtual identity of the machine. The authorization process at the stateful virtual identity machine can be as simple as considering an end user authorized simply by virtue of the fact that they have physically accessed the SVIM, as would be the case in a place where the SVIM is maintained in a secure

15   location and physical access is limited to only permitted users. Alternatively, the SVIM could include a table or tables and receive a key or keys of some number of bits in length from the end user device. The received key would be checked against the logical table and the end user would assume the identity of the machine if the received key or virtual identity character (VIC) matches any

20   content in the logical table in the SVIM.

Brief Description of the Drawings

FIG. 1 illustrates a schematic view of a prior art communication system.

FIG. 2 illustrates a schematic view of a system in which an embodiment of

25   the present invention may be incorporated.

FIG. 3 illustrates in block diagram form an element from the system of FIG. 2.

Detailed Description

30   The present invention is based on a different philosophy for managing access to resources. In contrast to the prior art systems where each individual server would maintain its own authorization capabilities, and in contrast to a co-

pending application by the present inventor, entitled "Method and Apparatus for Providing Centralized URL Authorization," based on Serial No. 60/113,493, filed on December 22, 1998, in which a centralized authentication facility is provided, the present invention is directed to a system in which authorization is provided by

5   some intermediate mechanism. In particular, it has been recognized that it is beneficial to provide one or more pre-authorized machines whereby the machine by nature of its identity is permitted access to various network resources which would be inaccessible given a different identifier. In accordance with the present invention, if any other user of the system is permitted to assume or is assigned the

10   identity of the pre-authorized machine, then that user will also have all of the access capabilities associated with the pre-authorized machine. In this way the present invention provides an element referred to as a stateful virtual identity machine (SVIM) which is pre-authorized to access network resources. An end user desiring to access the very same network resources can connect itself to the

15   SVIM, and, if the connection is allowed, the end user assumes the identity of the SVIM such that the connected end user has all of the access privileges assigned to the SVIM.

An example of a system in which the present invention may be deployed is illustrated in FIG. 2. This figure illustrates two servers, server A, 200 and server

20   B, 210. Both of the servers are connected to a wide area network (WAN) 250. A network node, a stateful virtual identity machine (SVIM) 240, is also connected to the wide area network. It should be noted that the term "connected" is intended to encompass direct and indirect connections so that it is possible for the servers or the SVIM to be connected into the wide area network via intermediate network

25   elements or nodes. The SVIM has a plurality of logical ports, here illustrated as ports 261 to 264. A work station 270, utilized by an end user, can be connected to one of the logical ports of the SVIM.

The SVIM is pre-authorized to have access to certain network resources. For example, perhaps the SVIM is associated with the service provider at server

30   A. That SVIM then may have access privileges to some or all of the resources of server A. In accordance with the present invention, the SVIM analyzes whether any of the devices which attempt to connect to one of its logical ports should be

allowed to do so. This can be done by checking a virtual identity characteristic (VIC) provided by the work station, for example, to the SVIM. In one embodiment, the VIC can be a key or work station identifier that is inserted in the layer-two headers of data transmission between the end user and the SVIM. These

5 VICs would be inserted either by the manufacturer of the end user machine, for example the work station or other devices such as a PC or cellular telephone, or could be inserted by software programs which are designed to synchronize end user VICs with VICs contained in the SVIM. If the SVIM in response to the VIC determines that the end user machine, here workstation 270, is allowed to connect

10 to the SVIM, then the end user assumes the virtual identity of the SVIM. Security profiles contained on security databases permit only those entities having the identity of the SVIM to access the resource. As a consequence, the SVIM can act as something of a concentrator of end user requests out in the network and can select those end users which will be permitted to assume the virtual identity of a

15 machine that is pre-authorized to have access to particular network resources. This configuration significantly reduces the load on security operations at the server itself and localizes security out in the network nearer to the end users seeking access to the network resources.

The SVIM are considered "stateful" in that in the configuration described

20 with respect to FIG. 2, the SVIM can remember whether a particular end user is connected to the SVIM or not. It keeps track of the "state" of the connection between any given end user and the SVIM.

An embodiment of the SVIM is shown in block diagram form in FIG. 3. The device includes a processor, CPU 320, operating under control of programs

25 stored in memory, such as VIC database 330. That same database can contain authorization information for implementing whether an end user can assure the virtual identity of the SVIM. The database can maintain authorization information in tabular form for example, such as in an access table that identifies whether a given user is authorized to assure the machine's identity. The table could correlate

30 user identifications with various resources, also having identifiers, accessible via the machine. Port 310 can be coupled to WAN as shown in FIG. 2 while ports

311 to 314 can correspond to ports 261 to 264 in FIG. 2. The ports, CPU and database can be coupled in an internal network configuration using a data bus 340.

Authorization of a given end user to assume the virtual identity of the SVIM may come from a more implicit activity than the exchange of keys or VIC

5   information. More specifically, it is possible that a particular SVIM may be positioned in a secure location such that only end users who have access to the secured location will be able to avail themselves of the use of the SVIM. In such a circumstance, it is the physical access to the SVIM which creates the presumption that the end user is an authorized user from the perspective of the

10   SVIM. Even in this circumstance, though, the end user, assumes the virtual identity of the SVIM for all purposes.

In this invention, then, the network resources do not worry about the true identity of the end user. Instead, all that is of significance to the network resource's security capabilities is that the end user has assumed the identity of the

15   SVIM to which it is logically or physically connected.

In accordance with the present invention, security capabilities localized with a server providing network resources can be modestly maintained by simply keeping track of the virtual identity machines which reside in the network and are pre-authorized to access network resources. The SVIM then assume the

20   responsibility, out in the connection points of the network, of identifying appropriate end users. If it is desirable to provide access for more users the additional SVIMs could be provided, the memory or logic tables of the SVIMs could be expanded or both.

This invention could have applicability not only in the context of services

25   providing, for example, web site or web page information, but in connection with other services which might be accessed via data networks. It is applicable in any environment in which an end user can be logically connected to a machine pre-authorized to have access to network resources and assume virtual identity of that machine.

30   The disclosed embodiments are illustrative of the various ways in which the present invention may be practiced. Other embodiments can be implemented

by those skilled in the art without departing from the spirit and scope of the present invention.

WHAT IS CLAIMED IS:

1.   A method for controlling access to network resources, the method comprising:

5   receiving at a network node, a request to assume the identity of the network node;

detecting whether the request originates with a user having a permissible virtual identity characteristic; and

if the user has a permissible virtual identity characteristic, sharing the

10   identity of the network node with the user, wherein network resources permit access to resources by the user as if it had the network node identity.

2.   A method for providing authorized access to a network resource, the method comprising:

15   receiving, at a preauthorized machine, from a first user a request to access a network resource;

detecting whether said first user is authorized to access said network resource; and

if said step of detecting indicates that said first user is authorized,

20   assigning the first user the identity of the preauthorized machine.

3.   The method of claim 2 further comprising:

receiving, at said preauthorized machine, from a second user a request to access a network resource detecting whether said second user is authorized to

25   access said network resource; and

if said step of detecting indicates that said second user is authorized, assigning the second user the identity of the preauthorized machine.

4.   The method of claim 3 wherein said first and second users are assigned

30   the identity of the preauthorized machine during overlapping time periods.

5. The method of claim 2 wherein said step of detecting includes,

receiving an identifier associated with the first user;

comparing the received identifier to a table of authorized identifiers; and

determining whether the received identifier matches any of the authorized

5   identifiers based on the results of the comparing operation.

6. The method of claim 2 wherein said step of detecting includes,

receiving a first identifier associated with the first user and a second identifier associated with a requested resource;

10   comparing the received first identifier/second identifier pair to contents of an authorized memory; and

determining that the user is authorized to access the requested resource if a match is found for the first and second identifier pair in the memory during the comparing step.

15

7. A method for providing access control with respect to assets available on a web server, the method comprising:

providing a plurality of machines authorized to access the web server;

associating with each authorized machine an access table storing

20   authorization information;

coupling one of the authorized machines to an access requester;

verifying that said requester is authorized to access an asset on the web server with reference to said access table associated with the authorized machine to which the requester is coupled; and

25   allowing the requester to assume the identity of said authorized machine to which the register is coupled after verifying that said requester is authorized.

8. The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of

30   assets at the web server and a second authorized machine that is authorized to access a second subset of assets at the web server, wherein said second subset differs from said first subset.

9. The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of assets at the web server and a second authorized machine that is authorized to

5   access a second subset of assets at the web server, wherein said second subset overlaps with said first subset.

10.   The method of claim 9 wherein said first and second subsets are identical.

10

113306
AWS 431

ABSTRACT OF THE DISCLOSURE

A method provides for control of access to network resources. A virtual identity machine resides in the network and is pre-authorized to access certain network resources. End users desiring access to those network resources attempt to logically connect to the virtual identity machines. If the logical connection attempt is successful, then the end user assumes the virtual identity of the virtual identity machine and has access to all of the same information that was available to the virtual identity machine.
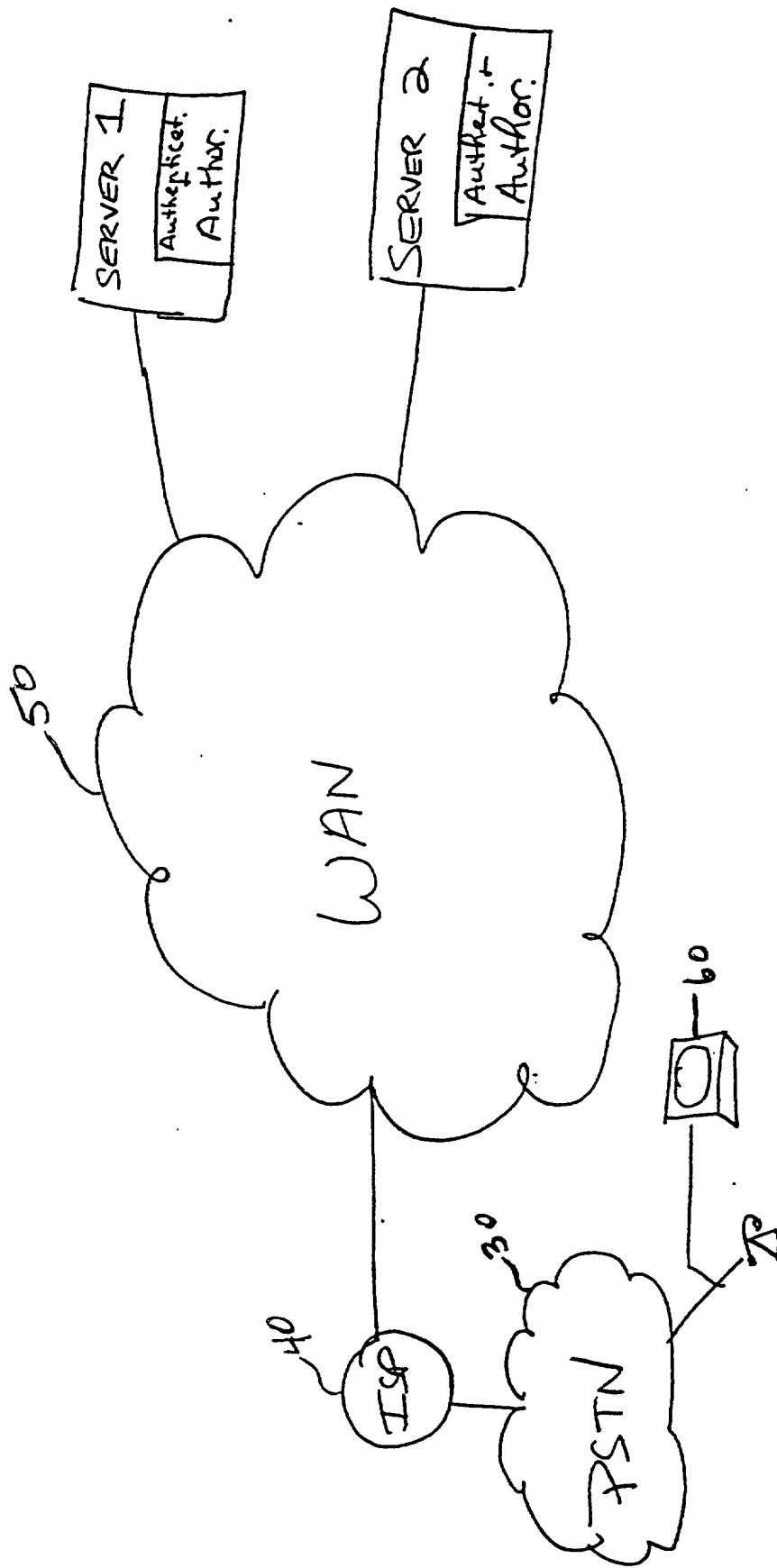
5

10

SERVER 1
Authenticat. Author.

SERVER 2
Authent.+ Author.

WAN

50

ISP 40

PSTN 30

60

20

FIG. 1
(Prior Art)

SERVER A

300

WORK STATION

270

261
262
263
264

240

SVMI

250

WAN

240

SERVER B

FIG. 2

SVM1

CPU 320

Port 310

340
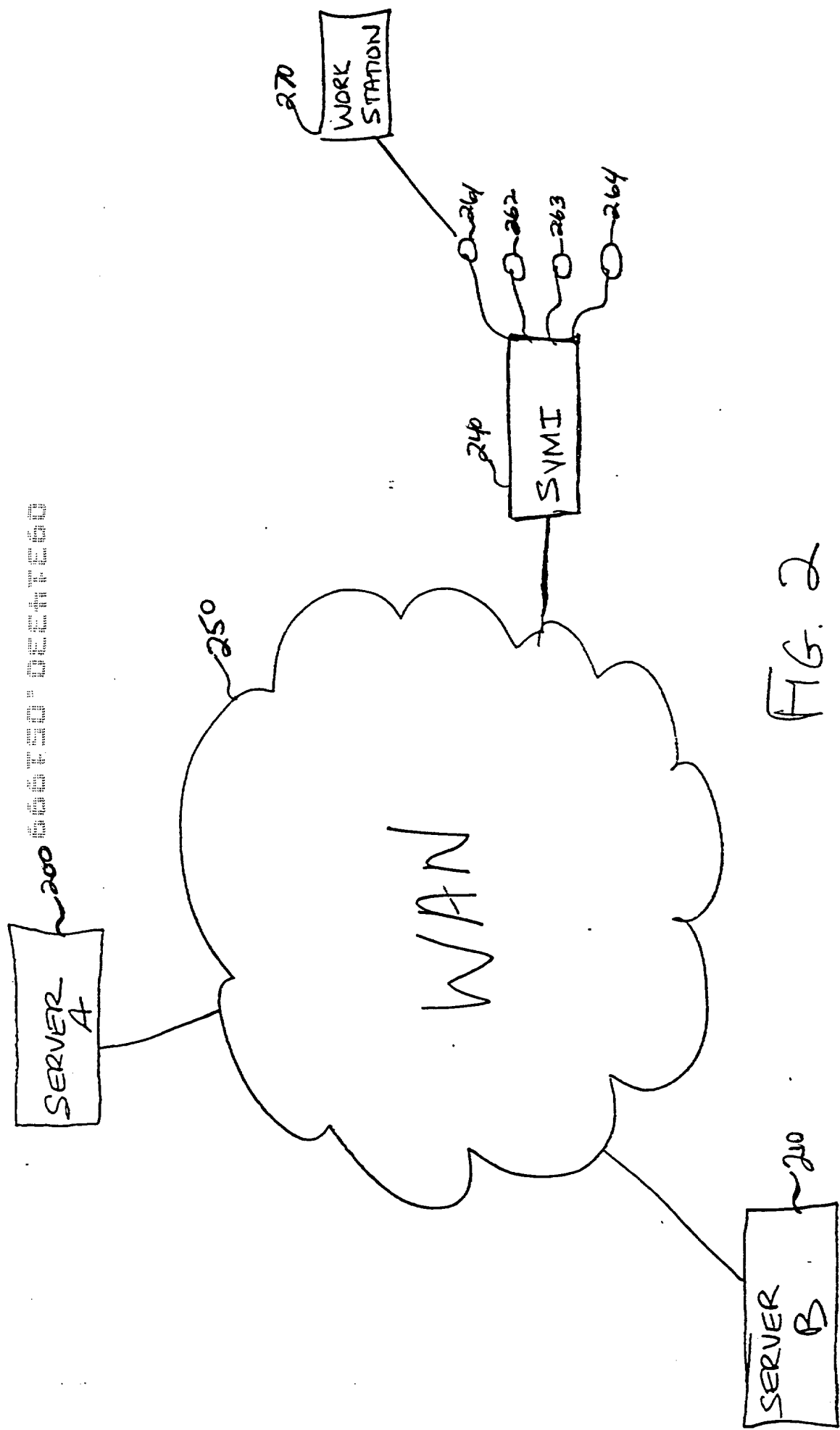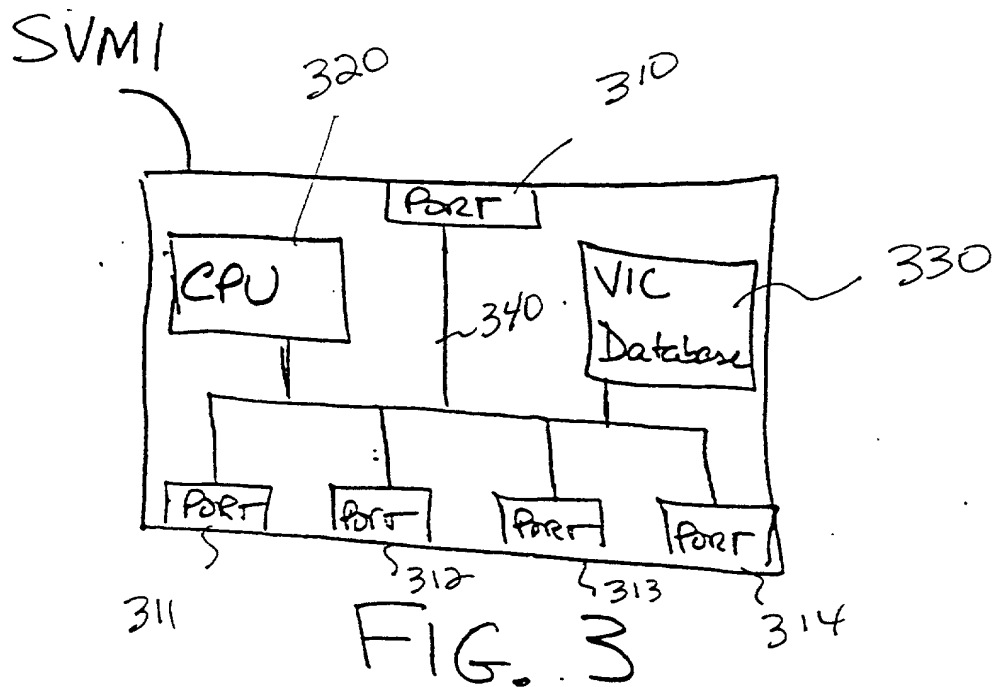
VIC Database 330

Port 311 Port 312 Port 313 Port 314

FIG. 3

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **System For Securing Inbound And Outbound Data Packet Flow In A Computer Network,** the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventors' certificate listed below and have also identified below any foreign application for patent or inventors' certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, we acknowledge the duty to disclose all information known to us to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. Provisional Application Serial No. 60/113,495, filed December 22, 1998

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Samuel H. Dworetsky	(Reg. No. 27873)
Thomas A. Restaino	(Reg. No. 33444)
Jose de la Rosa	(Reg. No. 34810)
Michele L. Conover	(Reg. No.34962)
Robert B. Levy	(Reg. No. 28234)
Benjamin S. Lee	(Reg. No. 42787)
Alfred G. Steinmetz	(Reg. No. 22971)

I also appoint Frank Pietrantonio (Reg. No. 32289) of Kenyon & Kenyon as associate attorney, with full power to prosecute said application, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

Please address all correspondence to Mr. S. H. Dworetsky, AT&T Corp., P.O. Box 4110, Middletown, New Jersey 07748. Telephone calls should be made to Samuel H. Dworetsky at 932-360-8120.

Full name of sole inventor: Arturo Maria

Inventor's signature _____ Date 5/18/99

Residence: Bellevue, King County, Washington

Citizenship: United States of America

Post Office Address: 2802 107th Avenue NE
                            Bellevue, Washington   98004